

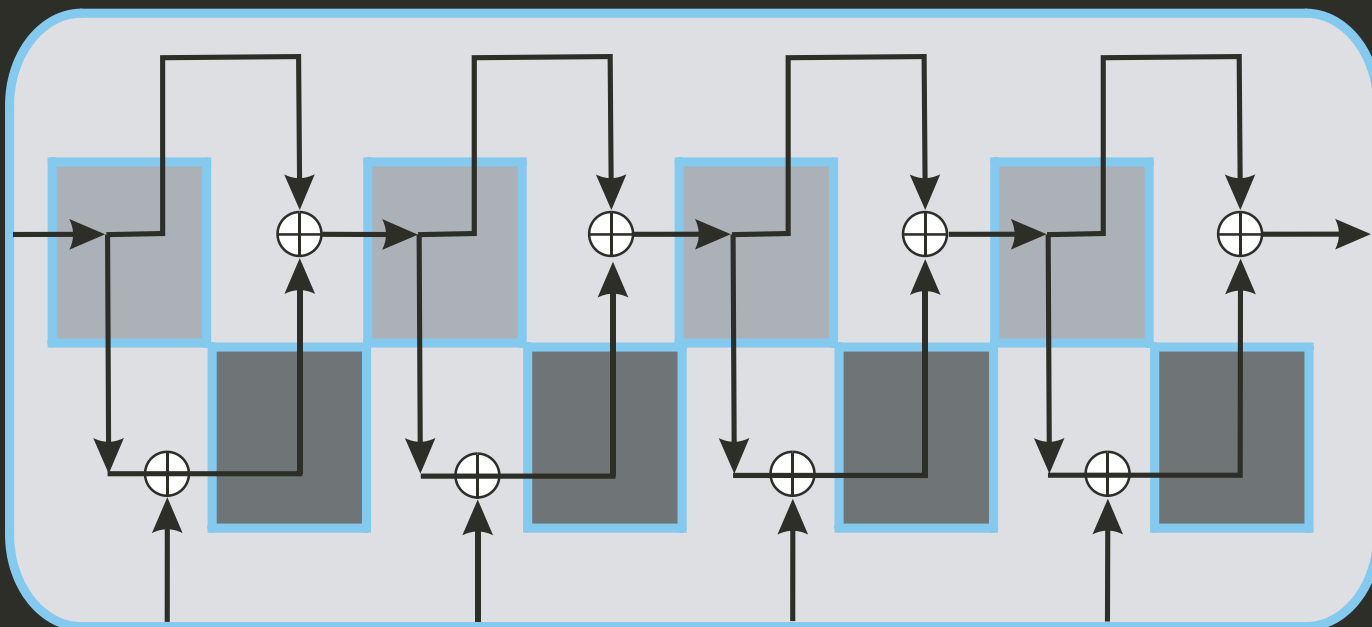
Journal of Research

of the

National Institute of Standards and Technology

May - June 2001, Vol. 106, No.3 ISSN 1044-677X

Advanced Encryption Standard Development Effort



NIST

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Available online
<http://www.nist.gov/jres>

The National Institute of Standards and Technology was established in 1988 by Congress to “assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries.”

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry’s competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency’s basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department’s Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering, and develops measurement techniques, test methods, standards, and related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST’s research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Publications and Program Inquiries Desk, 301-975-3058.

Office of the Director

- National Quality Program
- International and Academic Affairs

Technology Services

- Standards Services
- Technology Partnerships
- Measurement Services
- Information Services

Advanced Technology Program

- Economic Assessment
- Information Technology and Applications
- Chemistry and Life Sciences
- Materials and Manufacturing Technology
- Electronics and Photonics Technology

Manufacturing Extension Partnership Program

- Regional Programs
- National Programs
- Program Development

Electronics and Electrical Engineering Laboratory

- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Radio-Frequency Technology¹
- Electromagnetic Technology¹
- Optoelectronics¹

Materials Science and Engineering Laboratory

- Intelligent Processing of Materials
- Ceramics
- Materials Reliability¹
- Polymers
- Metallurgy
- NIST Center for Neutron Research

Chemical Science and Technology Laboratory

- Biotechnology
- Physical and Chemical Properties²
- Analytical Chemistry
- Process Measurements
- Surface and Microanalysis Science

Physics Laboratory

- Electron and Optical Physics
- Atomic Physics
- Optical Technology
- Ionizing Radiation
- Time and Frequency¹
- Quantum Physics¹

Manufacturing Engineering Laboratory

- Precision Engineering
- Manufacturing Metrology
- Intelligent Systems
- Fabrication Technology
- Manufacturing Systems Integration

Building and Fire Research Laboratory

- Applied Economics
- Structures
- Building Materials
- Building Environment
- Fire Safety Engineering
- Fire Science

Information Technology Laboratory

- Mathematical and Computational Sciences²
- Advanced Network Technologies
- Computer Security
- Information Access
- Convergent Information Systems
- Information Services and Computing
- Software Diagnostics and Conformance Testing
- Statistical Engineering

¹ At Boulder, CO 80303.

² Some elements at Boulder, CO.

Journal of Research of the **National Institute of** **Standards and Technology**

Volume 106

Number 3

May–June 2001

Board of Editors

Theodore V. Vorburger
Chief Editor

Available online
<http://www.nist.gov/jres>

Nancy M. Trahey, Technology Services

Loucas G. Christophorou, Electronics and Electrical Engineering Laboratory

Theodore V. Vorburger, Manufacturing Engineering Laboratory

Cynthia J. Zeissler, Chemical Science and Technology Laboratory

Ronald Collé, Physics Laboratory

Cynthia K. Montgomery, Materials Science and Engineering Laboratory

Nicos S. Martys, Building and Fire Research Laboratory

Alan H. Goldfine, Information Technology Laboratory

Daniel W. Lozier, Information Technology Laboratory

Clifton M. Carey, Paffenbarger Research Center

Julian M. Ives

Managing Editor, and Technical Production Editor

Ilse E. Putman, Karen J. Wick

Electronic Composition



U.S. Department of Commerce—**Donald L. Evans**, Secretary

Technology Administration—**Karen H. Brown**, Acting Under Secretary of Commerce for Technology

National Institute of Standards and Technology—**Karen H. Brown**, Acting Director

Cover: The cover illustration is symbolic of the Advanced Encryption Standard Development Effort at NIST. In 1997, NIST initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive (unclassified) Federal information. The research results and rationale for selection of the algorithm are documented in the article on p. 511 of this issue. Cover illustration arranged by C. Carey.

The *Journal of Research of the National Institute of Standards and Technology*, the flagship periodic publication of the national metrology institute of the United States, features advances in metrology and related fields of physical science, engineering, applied mathematics, statistics, and information technology that reflect the scientific and technical programs of the Institute. The *Journal* publishes papers on instrumentation for making accurate measurements, mathematical models of physical phenomena, including computational models, critical data, calibration techniques, well-characterized reference materials, and quality assurance programs that report the results of current NIST work in these areas. Occasionally, a Special Issue of the *Journal* is devoted to papers on a single topic. Also appearing on occasion are review articles and reports on conferences and workshops sponsored in whole or in part by NIST.

ISSN 1044-677X

Coden: JRITEF

Library of Congress Catalog Card No.: 89-656121

United States Government Printing Office, Washington: 2001

Contents

Available online
<http://www.nist.gov/jres>

Articles

Report on the Development of the Advanced Encryption Standard (AES)	James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and Edward Roback	511
Photocurrent Measurement of PC and PV HgCdTe Detectors	George P. Eppeldauer and Robert J. Martin	577
Treasure of the Past VII: Measurement of the Thickness and Refractive Index of Very Thin Films and the Optical Properties of Surfaces by Ellipsometry	Frank L. McCrackin, Elio Passaglia, Robert R. Stromberg, and Harold L. Steinberg	589

Conference Reports

Workshop on Texture in Electronic Applications	Mark D. Vaudin and Debra L. Kaiser	605
--	---	-----

News Briefs

GENERAL DEVELOPMENTS	609
NIST Develops Smart Space Test Bed New Fingerprint Standard Approved	
NIST's Biometric Data Format Endorsed by Industry NIST's Cryptographic Module Validation Program Adds First PDA Device	610
NIST Develops Metal Detector Emulator to Study Adverse Effects on Medical Devices NIST-Supported Standard Adopted by RosettaNet E-Commerce Consortium New Microscopy Capability at NIST	611
New High T_c Boron Superconductor Parallel Processing Enables Rapid Computation of X-Ray Absorption	612
NIST Scientists Ensure the Accuracy of Measurements Made by the Triana Satellite New Publications on the Fundamental Constants Algorithm Developed for Minimizing Cumulative Time-Base Quantization Errors	613

Evaluation of Electromagnetic Compatibility (EMC) Compliance Chambers LTCC Substrates Characterized at High Frequencies IEC Technical Committee, Led by NIST, Publishes Four New Superconductivity Standards	614
NIST Co-Sponsors Government-Industry IT Security Forum NIST Hosts Working Group Meeting on ITL Biometrics Initiative International Standards for Thermal Properties of Polymer Melts	615
At Conference, The “P” in PC Stands for “Pervasive” Paper Describes NIST Support for Optical Fiber Industry Conference Seeks IT Access for All	616
Practice Guide on Particle Size Characterization Now Available Paper Traces History of NIST Refrigerants Program	617
New Excimer Laser Measurement Service Available Third Patent for NIST’s Role-Based Access Control Work Non-Linear Optical Characterization of Gallium Nitride Aids Material Improvement	618
NIST’s Cryptographic Module Validation Program Adds Web Access for Security Policies NIST Web Metrics Testbed Released	619
NIST Advanced Radiometer Calibrated and Delivered to NASA Neutrons Used to Characterize a Novel Lithium-Containing Zeolite Researchers Develop New Transient Thermal Imaging System	620
Qualification of EMC Test Sites Ultracold Neutral Plasmas Created at NIST Thickness Variations Measured In Silicon Wafers New “Model” Function for SEM Images of Dense Lines	621
Improved Statistical Analysis Tool Preliminary Comparison Results of Nano3 Line Scales Shipped NIST a Sponsor of Second International Conference on Oxidative Stress and Aging	622
Digital Library of Mathematical Functions Profiles in Physics Publications NIST Takes Over as MPEG Web Site Host June Workshop Examines Draft Language for Materials Data Exchange	623
Group Wants to Make “E-Business” as Easy as “A-B-C” June Symposium Showcases Interactive Digital TV Microtester “Stresses” Electronic Packaging	624
Data Exchange Standards Advance History of Pioneering NIST Facility Chronicled	625
STANDARD REFERENCE MATERIALS High Resolution Wavelength Calibration SRM for Wavelength Division Multiplexing	626
